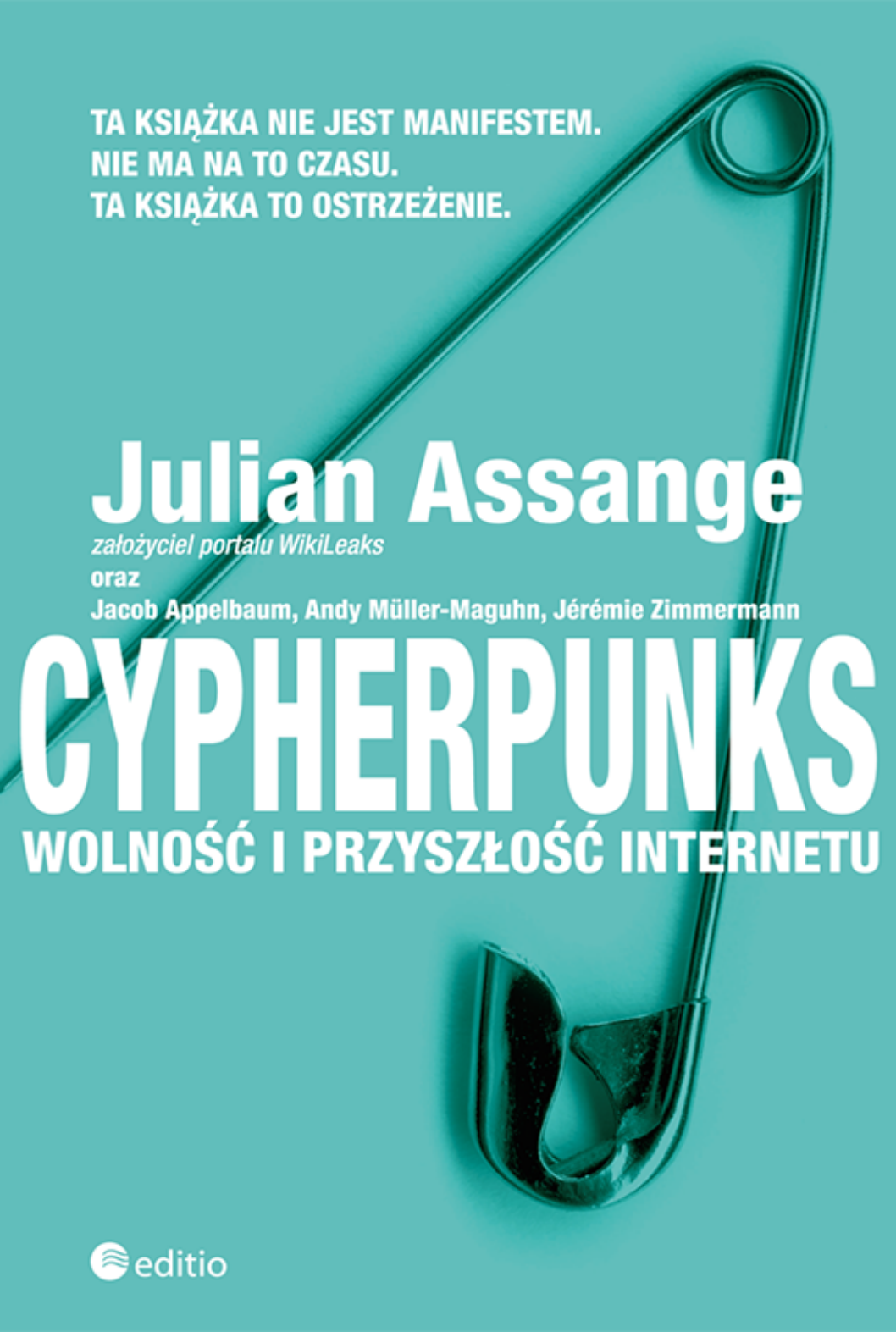
TA KSIĄŻKA NIE JEST MANIFESTEM.
NIE MA NA TO CZASU.
TA KSIĄŻKA TO OSTRZEŻENIE.
Julian Assange
założyciel portalu WikiLeaks
oraz
Jacob Appelbaum, Andy Müller-Maguhn, Jérémie Zimmermann
CYPHERPUNKS
WOLNOŚĆ I PRZYSZŁOŚĆ INTERNETU
editio

Tytuł oryginału: Cypherpunks

Tłumaczenie: Marcin Machnik
Projekt okładki: Anna Mitka

ISBN: 978-83-246-7325-4

First published by OR Books LLC, New York

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: editio@editio.pl
WWW: http://editio.pl (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Intensywniejsza komunikacja kontra intensywniejsza inwigilacja

JULIAN: Gdy wrócimy do momentu na początku lat dziewięćdziesiątych, gdy rodził się ruch cypherpunkowy w odpowiedzi na rządowe zakazy dotyczące kryptografii, mnóstwo ludzi przyglądało się możliwościom internetu w kwestii wolnej, niecenzurowanej komunikacji — w odróżnieniu od mediów głównego nurtu. cypherpunk jednak zawsze dostrzegał też to, że z tym wiąże się możliwość przechwytywania wszystkich komunikatów. Aktualnie żyjemy w czasach intensywniejszej komunikacji oraz intensywniejszej inwigilacji. Intensywniejsza komunikacja oznacza, że masz większy zakres wolności względem osób, które próbują kontrolować idee i fabrykować konsensus. Intensywniejsza inwigilacja to coś dokładnie przeciwnego.

Inwigilacja jest dzisiaj znacznie bardziej wyraźna niż w czasach, gdy była w głównej mierze sprawką Ameryki, Wielkiej Brytanii, Rosji i paru innych rządów, takich jak Szwajcaria i Francja. Teraz zajmują się tym chyba wszyscy — niemal każdy kraj — z powodu komercjalizacji masowego inwigilowania. Dodatkowo inwigilacja się totalizuje, gdyż ludzie przenoszą swoje poglądy polityczne, rozmowy rodzinne i znajomości do internetu. Mamy więc do czynienia nie tylko z intensywniejszą inwigilacją istniejącej komunikacji, lecz także ze znacznym zwiększeniem intensywności samej komunikacji.

Aktów komunikacji jest nie tylko więcej w znaczeniu ilościowym, lecz także rodzajowym. Wszystkie nowe typy komunikacji, które kiedyś były prywatne, dzisiaj są masowo przechwytywane.

Jest to konflikt między potęgą informacji zgromadzonych przez insiderów, tych nieformalnych zbieraczy informacji, którzy zaczynają się rozwijać, wymieniać danymi i tworzyć połączenia między sobą oraz z sektorem prywatnym, a wspólnymi wartościami w internecie jako społecznym medium ludzkości służącym do wyrażania siebie.

Chciałbym zastanowić się nad tym, jak przedstawiamy nasze idee. Moim największym problemem jako osoby zinwigilowanej do szpiku kości, która rozumie to, w jakim stopniu w ostatnich dwudziestu latach rozwinęła się branża transnarodowych sił bezpieczeństwa, jest to, że zbyt dobrze to wszystko znam i nie wiem, jak na to patrzeć z powszechnej perspektywy. Dzisiaj jednak nasz świat stał się światem każdego człowieka, ponieważ wszyscy wrzuciliśmy najważniejszą część swojego życia do internetu. Musimy w jakiś sposób przekazać sobie to, co wiemy, dopóki jest to możliwe.

ANDY: Sugeruję nie patrzeć na to z perspektywy obywatela, lecz osoby mającej władzę. Niedawno byłem na dziwnej konferencji w Waszyngtonie i poznałem gości z plakietkami ambasady niemieckiej. Podszedłem do nich i powiedziałem: „O, jesteście z ambasady niemieckiej", a oni odparli: „Ach, nie do końca z ambasady, jesteśmy z okolic Monachium". Okazało się, że byli z zagranicznego wywiadu. Zapytałem ich w trakcie wieczornego poczęstunku: „Co jest celem utajniania?". Odparli: „Cóż, chodzi o spowolnianie procesów, aby łatwiej je było kontrolować". To jest podstawowe zadanie wywiadu — spowolnienie procesów poprzez odbieranie ludziom możliwości ich zrozumienia. Ogłoszenie czegoś tajnym oznacza, że ograniczasz liczbę ludzi, którzy mają wiedzę umożliwiającą wpłynięcie na proces.

Jeśli spojrzysz na internet z perspektywy ludzi u władzy, ostatnie dwadzieścia lat było przerażające. Postrzegali internet jako chorobę, która upośledza ich przywilej definiowania rzeczywistości i tego, co się dzieje, co z kolei służyło do definiowania tego, co ludzie wiedzą, oraz ich możliwości interakcji z tym. Gdy spojrzysz na przykład na Arabię Saudyjską, gdzie przez jakiś historyczny przypadek liderzy religijni i ludzie posiadający większość

kraju to te same osoby, ich zainteresowanie zmianami jest równe zeru. A może nawet minus pięciu. W ich oczach internet jest chorobą, więc pytają swoich doradców: „Macie jakieś szczepionki na to, co się tu dzieje? Musimy być uodpornieni, gdy to coś, ten cały internet, dosięgnie naszego kraju". Odpowiedzią jest masowa inwigilacja, czyli: „Musimy całkowicie kontrolować internet, musimy go filtrować, musimy wiedzieć o wszystkim, co robią ludzie". I do tego właśnie doszło w ciągu ostatnich dwudziestu lat. W inwigilację zainwestowano potężne środki, gdyż ludzie u władzy bali się, że internet zmieni ich sposób sprawowania rządów.

JULIAN: A mimo tej masowej inwigilacji masowa komunikacja doprowadziła do tego, że miliony ludzi były w stanie dojść do szybkiego porozumienia. Jeśli da się bardzo szybko przejść od normalnego stanu do nowego stanu masowego porozumienia, to nawet jeśli władza widzi rozwój tej sytuacji, nie ma na tyle czasu, aby opracować skuteczną reakcję.

Muszę jednak powiedzieć o tym, jak w 2008 roku za pośrednictwem Facebooka zorganizowano protest w Kairze. Był on zaskoczeniem dla rządu Mubaraka, lecz uczestników wyśledzono za pomocą Facebooka[1]. W 2011 roku w instrukcji, która była jednym z najważniejszych dokumentów wykorzystanych w rewolucji egipskiej, na pierwszej stronie napisano, aby nie korzystać z Twittera ani Facebooka przy rozpowszechnianiu tej instrukcji; na ostatniej także napisano, żeby nie korzystać z Twittera ani Facebooka przy

[1] Był to protest przeprowadzony 6 kwietnia 2008 roku w ramach wsparcia dla stłumionego strajku pracowników firmy tekstylnej w Al-Mahalla al-Kubra. Na krótko przed strajkiem na Facebooku utworzono grupę „April 6 Youth Movement", która w zamyśle twórców miała zachęcać Egipcjan do protestowania w Kairze i innych miejscach w ramach wyrażania jedności z wydarzeniami w Mahalla. Protest nie przebiegł zgodnie z planem, a administratorzy grupy facebookowej Esraa Abdel Fattah Ahmed Rashid i Ahmed Maher zostali aresztowani wraz z innymi osobami. Mahera torturowano, aby wyjawił hasło do swojego profilu. April 6 Youth Movement działał dalej i odegrał rolę w rewolucji egipskiej z 2011 roku. Zobacz: *Cairo Activists Use Facebook to Rattle Regime*, „Wired", 20 października 2008 roku: *http://www.wired.com/techbiz/startups/magazine/16-11/ff_facebookegypt?current-Page=all* [dostęp: 23 października 2012].

rozpowszechnianiu tej instrukcji[2]. Mimo to bardzo wielu Egipcjan użyło w tym celu Twittera i Facebooka. Nic im się nie stało, gdyż rewolucja skończyła się sukcesem. Gdyby jednak się nie powiodła, ci ludzie znaleźliby się w bardzo, ale to bardzo ponurej sytuacji. Nie zapominajmy, że prezydent Mubarak dość szybko odciął dostęp do internetu. Trudno powiedzieć, czy brak dostępu do sieci ułatwił rewolucję, czy jej zaszkodził. Niektórzy myślą, że ją ułatwił, gdyż ludzie musieli wyjść na ulice, aby dowiedzieć się, co się dzieje, a gdy już wyjdziesz na ulicę, to będziesz na ulicy. Poza tym wszyscy poczuli się nękani, gdy przestały działać komórki i internet.

Aby więc rewolucja była skuteczna, musi zebrać masę krytyczną, musi się wydarzyć szybko i musi się skończyć powodzeniem, bo jeśli się nie powiedzie, to ta sama infrastruktura, która umożliwiła szybkie porozumienie, zostanie wykorzystana do wyśledzenia i odsunięcia na margines wszystkich osób zaangażowanych w namawianie do porozumienia.

To był Egipt, który oczywiście był sojusznikiem USA, lecz nie jest częścią angielskojęzycznego sojuszu wywiadów USA, Wielkiej Brytanii, Australii, Nowej Zelandii i Kanady. Spróbujmy sobie wyobrazić, że taka rewolucja wybucha nie w Egipcie, tylko w USA — co stałoby się z Facebookiem i Twitterem? Przejęłoby je państwo. I gdyby rewolucja się nie powiodła, zostałyby prześwietlone — tak jak robi się teraz — przez CIA i FBI w poszukiwaniu kluczowych uczestników.

JÉRÉMIE: Trudno oddzielić inwigilację od kontroli. Musimy się zająć obiema kwestiami. To mnie bardziej interesuje — kontrola internetu, i to niezależnie od tego, czy sprawują ją rządy, czy korporacje.

[2] Instrukcja „How to Protest Intelligently" anonimowego autora, dystrybuowana na początku osiemnastodniowego powstania, które doprowadziło do usunięcia prezydenta Mubaraka (arabskiego): *http://www.itstime.it/Approfondimenti/EgyptianRevolutionManual.pdf*. Niektóre fragmenty zostały przetłumaczone na angielski i opublikowane jako *Egyptian Activists' Action Plan: Translated*, „Atlantic", 27 stycznia 2011 roku: *http://www.theatlantic.com/international/archive/2011/01/egyptianactivists-action-plan-translated/70388* [dostęp do obu linków: 23 października 2012].

JACOB: Myślę, że to dość oczywiste, iż cenzura jest produktem ubocznym samej inwigilacji — zarówno autocenzura, jak i faktyczna cenzura proceduralna. Moim zdaniem ważne jest to, aby przekazać to ludziom w nietechniczny sposób. Na przykład tak: gdybyśmy budowali drogi w taki sposób, jak budujemy połączenia w internecie, każda droga musiałaby być wyposażona w kamery i mikrofony inwigilujące, do których dostęp miałaby wyłącznie policja lub ktoś skutecznie udający policjanta.

JULIAN: Jake, tutaj, w Wielkiej Brytanii, zmierzamy do tego.

JACOB: Gdy budujesz drogę, nie ma wymogu, żeby każdy jej cal był monitorowany przez doskonały system inwigilacyjny dostępny tylko dla tajnej grupy ludzi. Trzeba wyjaśnić zwykłym ludziom, że w ten sposób budujemy połączenia w internecie i każemy ludziom z nich korzystać — bo to jest coś, do czego normalny człowiek jest w stanie się odnieść, gdy uświadomi sobie, że budowniczowie infrastruktury nie zawsze będą tymi, którzy ją kontrolują.

ANDY: Ale niektórzy nawet nie budują dróg. Zakładają ogród i zachęcają ludzi do rozbierania się. Mówimy tu o Facebooku! Jego biznesowym zadaniem jest sprawienie, aby ludzie czuli się komfortowo, ujawniając swoje dane.

JACOB: Dokładnie. Ludzie dostali rekompensaty za to, że byli w Stasi — służbach bezpieczeństwa NRD — i dostają rekompensaty za uczestniczenie w Facebooku, tyle że na Facebooku otrzymują kredyt społeczny — uda im się przespać z sąsiadką — a nie bezpośrednie korzyści finansowe. Ważne jest powiązanie tego z aspektem ludzkim, gdyż nie chodzi tu o technologię, tylko o kontrolę poprzez inwigilowanie. W pewnym sensie jest to idealny Panoptikon[3].

[3] Panoptikon to wymyślone w 1787 roku przez filozofa Jeremiego Benthama więzienie, w którym jeden strażnik mógłby niepostrzeżenie obserwować wszystkich więźniów jednocześnie, mając ich na linii wzroku. Jeremy Bentham, *The Panopticon Writings*, red. Miran Bozovic, Verso 1995, dostępna online: *http://cartome.org/panopticon2.htm* [dostęp: 22 października 2012].

JULIAN: Interesuję się trochę filozofią technologii. Technologia oznacza nie tylko coś technicznego, lecz także na przykład większościowe porozumienie na zebraniu lub strukturę parlamentu — technologia to usystematyzowana interakcja. Na przykład wydaje mi się, że system feudalny wyniknął z technologii młyna. Po scentralizowaniu młynów, które wymagały potężnych inwestycji i były łatwe do fizycznego kontrolowania, system neutralny był całkiem naturalną konsekwencją. Wraz z upływem czasu można zaobserwować pojawianie się coraz bardziej wyszukanych technologii. Niektóre z nich można zdemokratyzować i przekazać wszystkim ludziom. Większość z nich jednak z racji swej złożoności formuje się w silnie powiązanych wewnętrznie organizacjach, takich jak Intel Corporation. Być może naturalne dla technologii jest przechodzenie przez te okresy: odkrywanie, centralizowanie i demokratyzowanie, które ma miejsce wtedy, gdy wiedza o niej zaleje następne, wyedukowane pokolenie. Myślę jednak, że generalną tendencją dla technologii jest jej scentralizowane kontrolowanie przez te osoby, które panują nad fizycznymi zasobami związanymi z technologią.

Skrajnym przykładem tego zjawiska jest coś takiego jak fabryka półprzewodników; wymaga ona takiego porządku, że nawet powietrze musi być czyste, oraz taśm montażowych z tysiącami ludzi noszącymi siatki na włosy, aby żaden kawałek skóry czy włos nie zakłóciły procesu produkcyjnego, który jest wieloetapowy i niewiarygodnie skomplikowany. A organizacja produkująca przewodniki jest w posiadaniu wiedzy liczonej dosłownie w milionach godzin badań. Jeśli te produkty są popularne — a są — i stanowią podporę internetu, to z wyzwoleniem internetu nieodzownie wiąże się produkowanie półprzewodników. A z produkcją półprzewodników wiąże się możliwość wymuszania ogromnych ustępstw przez tego, kto ma fizyczną kontrolę nad tą produkcją.

Tak więc podporą rewolucji w technologiach komunikacyjnych — i wolności, jaką dzięki temu uzyskaliśmy — jest cała neoliberalna, transnarodowa i zglobalizowana ekonomia nowoczesnych rynków. To tak naprawdę tylko wierzchołek. W kategoriach osiągnięć technologicznych jest to maksimum tego, co nowoczesna zglobalizowana neoliberalna ekonomia jest w stanie wytworzyć. Fundamentem internetu są niewiarygodnie skomplikowane interakcje handlowe między producentami włókien światłowodowych, producen-

tami półprzewodników, kopalniami wydobywającymi te wszystkie zasoby a także finansowymi lubrykantami doprowadzającymi do dobicia targu, sądami egzekwującymi prawo własności prywatnej itd. Dlatego internet jest wierzchołkiem piramidy całego systemu neoliberalnego.

ANDY: Jeśli mowa o technologii, gdy Jan Gutenberg wynalazł prasę drukarską, była zakazywana w różnych regionach Niemiec, co przyczyniło się do jej rozpowszechnienia w całym kraju, ponieważ zakaz w jednym miejscu wymuszał przeniesienie się pod inną jurysdykcję[4]. Nie zgłębiałem wszystkich szczegółów tego tematu, lecz wiem, że to doprowadziło do zatargu z kościołem katolickim, gdyż złamało jego monopol na wydawanie książek, a gdy ekipa Gutenberga popadała w kłopoty prawne, przenosiła się gdzieś, gdzie nie było jeszcze zakazu. W pewien sposób sprzyjało to rozpowszechnianiu wynalazku.

Internet to nieco inny przypadek, bo z jednej strony dysponujesz maszyną, którą można wykorzystać jako narzędzie produkcyjne — w pewnym sensie był nią nawet Commodore 64, gdyż większość osób używała go do własnych celów.

JULIAN: Czyli że każda maszyna, jaką posiadasz, pozwala Ci uruchamiać własne oprogramowanie.

ANDY: Tak. Możesz też jej użyć do rozpowszechniania idei. Jednak z drugiej strony, filozoficznej — jak na początku lat dziewięćdziesiątych stwierdził John Gilmore, jeden z założycieli amerykańskiej organizacji Electronic Frontier Foundation, gdy internet stał się kwestią globalną — „Sieć postrzega cenzurę jako uszkodzenie i znajduje drogę naokoło”[5]. Jak wiemy dzisiaj,

[4] Jan Gutenberg (1398 – 1468) był niemieckim kowalem, który wynalazł druk mechaniczny ruchomą czcionką. Ten wynalazek doprowadził do jednego z najbardziej znaczących wstrząsów społecznych w historii. Jest to najbliższa historyczna analogia do wymyślenia internetu.

[5] John Gilmore jest jednym z założycieli cypherpunku, aktywistą wolności społecznych i założycielem Electronic Frontier Foundation. Fraza zacytowana przez Andy’ego została zaczerpnięta z artykułu: *First Nation in Cyberspace*, „Time

stwierdzenie to było wynikiem połączenia technicznej interpretacji z optymistycznym punktem widzenia, czyli swego rodzaju myślenia życzeniowego, a jednocześnie w pewnym sensie samospełniającej się przepowiedni.

JULIAN: Było to jednak prawdą w odniesieniu do Usenetu, który jest systemem mailowym łączącym wiele osób z wieloma osobami i został zainicjowany jakieś trzydzieści lat temu. Aby w prosty sposób wyjaśnić jego działanie, wyobraź sobie, że nie ma różnicy między ludźmi i serwerami, a każda osoba prowadzi własny serwer Usenetu. Piszesz coś i przekazujesz to jednej osobie lub dwóm. One (automatycznie) sprawdzają, czy już to mają u siebie. Jeśli nie, pobierają to i dają każdemu, z kim są połączone. I tak dalej. W efekcie wiadomość rozchodzi się wśród wszystkich i w końcu każdy dostaje jej kopię. Jeśli jakaś osoba zacznie to cenzurować, zostanie zignorowana i nic się nie zmieni. Wiadomość i tak rozprzestrzeni się wśród osób, które nie są cenzorami. Gilmore mówił o Usenecie, a nie o internecie. Nie miał też na myśli stron internetowych.

ANDY: Chociaż jest to technicznie poprawne, interpretacja jego słów oraz ich długoterminowy wpływ miały wygenerować ludzi, którzy rozumieją siebie oraz internet. Ludzie mówili: „OK, tutaj jest cenzura, obejdziemy ją", gdy polityk bez wiedzy technicznej myślał: „O cholera, pojawiła się nowa technologia, która ogranicza naszą kontrolę nad przestrzenią informacyjną". Myślę więc, że Gilmore, który był jednym z proroków cypherpunku, wykonał niezłą robotę, kierując sprawy w tę stronę. Zainspirowało to całą kryptograficzno-anarchistyczną metodę tworzenia własnych form anonimowej komunikacji, bez obaw, że ktoś będzie cię obserwował.

JÉRÉMIE: Dostrzegam różnicę w tym, co opisaliśmy jako rozprzestrzenianie się technologii. W przypadku młyna i prasy drukarskiej musiałeś spojrzeć na dane urządzenie, aby zrozumieć jego działanie, podczas gdy teraz coraz częściej umieszczamy kontrolę w obrębie technologii. Kontrola jest wbudowana. Jeśli przyjrzysz się współczesnym komputerom, w większości przy-

Magazine", 6 grudnia 1993 roku. Sprawdź stronę Johna Gilmore'a: *http://www.toad.com/gnu* [dostęp: 22 października 2012].

padków nawet nie jesteś w stanie ich otworzyć, aby poznać komponenty. A wszystkie komponenty znajdują się w małych obudowach i nie można zobaczyć, co robią.

ANDY: Ze względu na poziom skomplikowania?

JÉRÉMIE: Ze względu na poziom skomplikowania, lecz także z racji tego, że sama technologia w zamierzeniu nie ma być zrozumiała. Tak to wygląda w przypadku technologii zastrzeżonych prawnie[6]. Cory Doctorow opisuje to w artykule *The War on General Purpose Computing*[7]. Gdy komputer jest ogólną maszyną, możesz z nim zrobić wszystko. Możesz przetworzyć dowolną informację jako dane wejściowe i przekształcić ją na wyjściu w cokolwiek. A my tworzymy coraz więcej urządzeń, które mają w sobie normalny komputer, lecz ograniczony do bycia tylko GPS-em, telefonem lub odtwarzaczem MP3. Powstaje też coraz więcej urządzeń z wbudowanym systemem kontroli, który zabrania użytkownikowi wykonywania określonych działań.

JULIAN: Wbudowanym systemem kontroli, który ma nie pozwolić ludziom zrozumieć urządzenie i zmodyfikować go, aby służyło do innych celów, niż chciał producent, ale dzisiaj jest jeszcze gorzej, bo te urządzenia są podłączone do sieci.

[6] „Zastrzeżone technologie to dowolnego rodzaju systemy, narzędzia lub procesy techniczne, które zostały opracowane przez konkretne jednostki biznesowe i dla tych jednostek… Idee opracowane i przedłożone przez podwładnych są zazwyczaj uważane za własność intelektualną pracodawcy, przez co można im nadać status technologii zastrzeżonej". Definicja zaczerpnięta z wiseGEEK (w tłum. własnym — *przyp. tłum.*): *http://www.wisegeek.com/what-is-proprietary-technology.htm* [dostęp: 22 października 2012].

[7] Cory Doctorow, *The coming war on general-purpose computing*, boingboing, 10 stycznia 2012 roku (bazujący na przemówieniu wprowadzającym wygłoszonym na Chaos Computer Congress w grudniu 2011 roku): *http://boingboing.net/2012/01/10/lockdown.html* [dostęp: 15 października 2012].

JÉRÉMIE: Tak, dzięki czemu może zawierać funkcję monitorowania użytkownika i jego danych. To dlatego wolne oprogramowanie jest tak istotne dla wolnego społeczeństwa.

ANDY: Całkowicie zgadzam się z tym, że potrzebujemy maszyn ogólnego zastosowania, lecz dzisiaj rano, gdy miałem lecieć tutaj z Berlina, samolot przerwał startowanie — coś takiego zdarzyło mi się po raz pierwszy. Samolot zjechał na bok i kapitan obwieścił: „Panie i panowie, mamy błąd w systemach elektrycznych, więc postanowiliśmy się zatrzymać i zrestartować te systemy". Pomyślałem wtedy: „O cholera, to brzmi jak restartowanie Windowsa, Control+Alt+Delete — może zadziała!". Dlatego wcale bym się nie zmartwił, gdyby na samolocie były urządzenia do pojedynczych celów, które mają jedną funkcję i wykonują ją wyśmienicie. Gdy siedzę w latającej maszynie, nie chcę, żeby piloci rozpraszali się graniem w Tetris albo żeby ich komputery miały robaka Stuxnet czy cokolwiek innego[8].

JÉRÉMIE: Samolot sam z siebie nie przetwarza Twoich osobistych danych, nie ma kontroli nad Twoim życiem.

[8] Stuxnet to bardzo skomplikowany robak komputerowy, na temat którego panuje przekonanie, że został rozpowszechniony przez USA i Izrael w celu zaatakowania sprzętu firmy Simens, rzekomo używanego przez Iran do wzbogacania uranu. Krótki opis tego robaka znajdziesz w Wikipedii: *http://pl.wikipedia.org/wiki/Stuxnet*. Zobacz także: *WikiLeaks: US advised WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank*, „Guardian", 18 stycznia 2011 roku: *http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear*. WikiLeaks opublikowało jeden z najwcześniejszych raportów o zdarzeniu przypisywanym aktualnie robakowi Stuxnet — wypadku nuklearnym w ośrodku jądrowym Natanz w Iranie. Zobacz: *Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation*, WikiLeaks, 17 czerwca 2009 roku: *http://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief%27s_mystery_resignation*. Opublikowane przez WikiLeaks dowody pochodzące z globalnej korporacji inwigilującej Stratfor sugerują zaangażowanie Izraela. Zobacz: Email ID 185945, The Global Intelligence Files: *http://wikileaks.org/gifiles/docs/185945_re-alpha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html* [dostęp do wszystkich linków: 16 października 2012].

ANDY: Nie całkiem, latająca maszyna ma przecież kontrolę nad moim życiem na czas lotu.

JACOB: Argument Cory'ego najlepiej moim zdaniem opisać w ten sposób, że dzisiaj już nie ma samochodów, samolotów czy aparatów słuchowych; zamiast tego są komputery z czterema kołami, komputery ze skrzydłami i komputery, które pomagają słyszeć. Nie ma znaczenia, czy są to komputery jednozadaniowe, czy nie; ważne jest to, żebyśmy potrafili sprawdzić, czy wykonują zadanie, jakie mają wykonywać, oraz rozumieli, na ile dobrze to robią. Ludzie często próbują dowieść, że mają prawo zamykać dostęp do tej wiedzy i utrzymywać ją w tajemnicy, więc komplikują budowę komputerów lub sprawiają, że prawo utrudnia ich zrozumienie. To jest naprawdę niebezpieczne dla społeczeństwa, bo ludzie nie zawsze działają w najlepszym interesie wszystkich oraz zdarza im się popełniać błędy — nie ze złośliwości — więc zamykanie dostępu do tej wiedzy jest bardzo groźne na wielu poziomach, a jednym z istotniejszych jest nasza wrodzona niedoskonałość. To po prostu fakt. Dostęp do projektów systemów stanowiących podstawę naszego życia to jeden z powodów, dla których wolne oprogramowanie jest ważne. Zwiększa naszą umiejętność wprowadzania trwałych inwestycji, ulepszania używanych przez nas systemów oraz sprawdzania, czy działają zgodnie z oczekiwaniami.

Jednak niezależnie od wolności, zrozumienie tych systemów jest też ważne dlatego, że gdy ich nie rozumiemy, mamy tendencję do zdawania się na autorytety; na ludzi, którzy je rozumieją lub są w stanie je kontrolować, nawet jeśli wcale nie rozumieją istoty danego systemu. To dlatego jest tyle hałasu o cyberwojnę — bo ludzie, którzy wydają się mieć autorytet w sprawie wojny, zaczynają się wypowiadać o technologii tak, jakby ją rozumieli. Tacy ludzie często mówią o cyberwojnie, ale żaden z nich — ani jeden — nie mówi o budowaniu cyberpokoju ani czymkolwiek związanym z pokojem. Ich słowa zawsze dotyczą wojny, bo tym się zajmują. Próbują przejąć kontrolę nad procesami technologicznymi i prawnymi, aby zyskać narzędzia do promowania własnych interesów. Gdy więc nie mamy kontroli nad naszą technologią, tacy ludzie chcą jej użyć do własnych celów, a konkretnie do wojny. To jest recepta na różne przerażające scenariusze — myślę, że z tego powodu

powstał robak Stuxnet — a rozsądni w innych kwestiach ludzie sugerują, że chociaż USA prowadzi wojny, to taka taktyka w jakiś sposób im zapobiega. To mógłby być sensowny argument w przypadku kraju, który nie najeżdża innych nacji, lecz jest wysoce niewiarygodny w kontekście państwa zaangażowanego w wiele równoczesnych inwazji.

CYPHERPUNKS

WOLNOŚĆ I PRZYSZŁOŚĆ INTERNETU

Sieć daje wolność, sieć wolność zabiera

Internet zmienił świat. Przekształcił go w globalną wioskę, przyspieszając przepływ informacji na niespotykaną wcześniej skalę. Obywatelom dał moc obalania dyktatorów, wyborcom — siłę do demaskowania politycznych demagogów, a konsumentom — wiedzę niezbędną do śledzenia oszustów gospodarczych. Niestety, każdy kij ma dwa końce. W ciemnych zakamarkach globalnej sieci kryją się ludzie, rządy i korporacje, dla których informacje, jakie internet przechowuje o nas — zwykłych ludziach — stanowią potencjalną broń. Internet, najlepsze narzędzie służące wyzwoleniu, stał się najniebezpieczniejszym pomocnikiem totalitaryzmu, z jakim kiedykolwiek mieliśmy do czynienia.

Czy możemy się przed tym bronić?

Ruch *cypherpunk* to aktywiści promujący masowe korzystanie z silnej kryptografii jako sposobu na zabezpieczenie podstawowej wolności przed tym zaciekłym atakiem. Julian Assange, wizjoner i redaktor naczelny WikiLeaks, od lat dziewięćdziesiątych ubiegłego wieku jest głównym przedstawicielem tego środowiska. Teraz, na potrzeby tej ważnej i pojawiającej się w kluczowym momencie książki, Assange zebrał grupę rewolucyjnych myślicieli i aktywistów z pierwszej linii frontu walki o cyberprzestrzeń, by wspólnie dyskutować o tym, czy internet ostatecznie nas wyzwoli, czy zniewoli.

Przyłącz się do dyskusji i działaj, zanim będzie za późno!

Nr katalogowy: 14367

Księgarnia internetowa:
http://editio.pl

Zamówienia telefoniczne:
0 801 339900
0 601 339900

editio
Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: editio@editio.pl
http://editio.pl

Cena: 34,90 zł
ISBN 978-83-246-7325-4

9 788324 673254